UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/821,937	04/12/2004	Moon-jeong Choi	Q79284	2145

23373 7590 10/16/2008

SUGHRUE MION, PLLC
2100 PENNSYLVANIA AVENUE, N.W.
SUITE 800
WASHINGTON, DC 20037

EXAMINER	
KRISHNAN, VIVEK V	

ART UNIT	PAPER NUMBER
2445	

MAIL DATE	DELIVERY MODE
10/16/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/821,937	CHOI ET AL.	
	Examiner	Art Unit	
	VIVEK KRISHNAN	2445	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 July 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is responsive to the Amendment/Arguments filed on July 2, 2008. Claims 1-20 are pending.

Response to Arguments

1. Applicant's arguments with respect to Claim Objections due to informalities have been fully considered and are persuasive. The objection to Claim 9 has been withdrawn.

2. Applicant's arguments with respect to Claim Rejections under 35 U.S.C. 103 have been fully considered but they are not persuasive.

As to arguments with respect to Claim 1:

a. Page 10 - "With respect to independent claim 1, Applicants submit that neither Weiss nor Zelig, either alone or in combination, disclose or suggests at least, "wherein, if a registration request is transferred through an identifier based on registration rules provided for a registration of at least one of the external home networks from a multi-home service application built into the information devices connected to the at least one of the extemal home networks, the control unit maps the requested at least one of the external home networks and the identifier into the database," as recited in amended claim 1."

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically

pointing out how the language of the claims patentably distinguishes them from the references.

Furthermore, Applicant has failed to address secondary reference Jung, which was used reject limitations incorporated into amended Claim 1 in the Non-Final Rejection dated April 2, 2008. Amended Claim 1 is unpatentable over Weiss, Zelig, and Jung as rejected below.

As to arguments with respect to Claim 14:

b. Page 13 - "According to Applicants' review of the cited portion of Zelig, Zelig only describes routing multicast packets to a particular multicast group, which includes various destination nodes in the VPN to which a packet should be forwarded. However, nowhere does Zelig disclose or suggest the specific feature that if multicast packets are transferred to one of the external home networks through the VPN, the middleware processing unit forwards the multicast packets to the information devices connected to the home network."

As rejected below, Zelig discloses if multicast packets are transferred to an external network through a VPN, a router (middleware processing unit) forwards the multicast packets to the multicast group or nodes connected to the external network.

As to arguments with respect to Claims 2-20:

Applicant's arguments are moot in view of the aforementioned argument that Weiss, Zelig, and Jung disclose each and every limitation of Claim 1.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Application Publication No. 2002/0144144 A1 to Weiss et al. (hereinafter "Weiss") (IDS submitted June 9, 2006), and further in view of U.S. Patent No. 7,339,929 B2 to Zelig et al. (hereinafter "Zelig") and U.S. Patent Application Publication No. 2002/0129150 A1 to Jung.

5. As to Claim 1, Weiss discloses a multi-home service system, comprising:

a first interface for exchanging data with information devices connected to a home network (Weiss; Figure 1, discloses an interface for exchanging data with information devices connected to a network);

a second interface for exchanging data with other information devices connected to external home networks (Weiss; Figure 1, discloses an interface for exchanging data with information devices connected to external networks);

a storage unit for storing a database which is established based on information collected with respect to the information devices connected to the home network and other devices connected to the external home networks (Weiss; paragraphs 9-12 and 31-33, discloses a

database that includes information collected with respect to users and devices on the network and users and devices on external networks); and

a control unit for collecting information on the information devices connected to the home network and said other information devices, and providing a service for mutual accesses among the information devices connected to the home network and other information devices, registering the external networks in a database based on setup information on the external home networks that is transferred through the first interface [...] (Weiss; paragraphs 9-12 and 24-35, discloses collecting information on devices connected to the network and devices connected to external networks, providing mutual access among the devices on the networks, and registering users and devices on the external networks on a database based on setup information), and

[...] the control unit maps the requested at least one of the external home networks and the identifier into the database (Weiss; paragraphs 9-12 and 31-33, discloses mapping identifier and external network information into a database).

Weiss does not explicitly disclose, however Zelig discloses if multicast packets are delivered from the information devices connected to the home network and the other devices connected to the external home networks, delivering the multicast packets through a virtual private network (VPN) tunnel to the external home networks registered in database (Zelig; column 4 lines 30-53, discloses delivering received multicast packets through a VPN tunnel to external networks).

It would have been obvious to one of ordinary skill in the art to modify a control unit for providing mutual access among devices on different networks, as disclosed by Weiss, to include

delivering received multicast packets through a VPN tunnel to external networks, as disclosed by Zelig, in order to provide multicast capability to nodes that are part of a VPN (Zelig; column 4 lines 30-53).

Weiss does not explicitly disclose, however Jung discloses storing identifier and external network information if a registration request is transferred through an identifier based on registration rules provided for a registration of at least one of the external home networks from a multi-home service application built into the information devices connected to the at least one of the external home networks (Jung; Table 1, paragraph 49, and Figures 5 and 12, discloses storing identifier and external network information in response to a request to register with a VPN in accordance with a registration request format).

It would have been obvious to one of ordinary skill in the art to modify mapping identifier and external network information into a database, as disclosed by Weiss, such that the mapping is performed in response to a request, as disclosed by Jung, in order to provide VPN services to an external network or device upon request to register (Jung; paragraph 49).

6. As to Claim 2, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 1. Weiss further discloses wherein the control unit comprises:

an application processing unit for receiving and transferring messages with a multi-home service application built therein in order for the information devices connected to the home network to be set up with accesses to and information on the external home networks (Weiss;

paragraphs 9-12 and 31-33, discloses collecting information on a database in order to allow devices on a network access to devices on external networks);

a network processing unit for forming the VPN tunnel through Communications with gateways of the external home networks, and processing mutual data exchanges with the other information devices connected to the external home networks through the VPN tunnel (Weiss; paragraphs 9-12 and 24-35, discloses forming a VPN tunnel and processing mutual data exchanges with devices on external networks); and

a main processing unit for collecting information on the information devices connected to the home network and the other information devices, providing a service for mutual accesses among the information devices and the other information devices (Weiss; paragraphs 9-12 and 24-35, discloses collecting information on devices connected to the network and devices connected to external networks, and providing mutual access among the devices on the networks), and

Weiss does not explicitly disclose, however Zelig discloses if the multicast packets are transferred from the information devices connected to the home network, processing multicast packet transfers through the VPN tunnel formed through the network processing unit (Zelig; column 4 lines 30-53, discloses delivering received multicast packets through a VPN tunnel to external networks).

It would have been obvious to one of ordinary skill in the art to modify providing mutual access among devices on different networks, as disclosed by Weiss, to include delivering received multicast packets through a VPN tunnel to external networks, as disclosed by Zelig, in

order to provide multicast capability to nodes that are part of a VPN (Zelig; column 4 lines 30-53).

7. As to Claim 3, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 2. Weiss further discloses wherein the application processing unit comprises:

an external home network list providing unit for, if the multi-home service application requests a list of external home networks registered, providing the list with reference to the database (Weiss; paragraph 31, discloses the database is a relational database built on SQL such that if an application requests a list of networks registered on the database, the list is provided with reference to the database).

8. As to Claim 4, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 3. Weiss further discloses wherein the application processing unit further comprises:

a second registration unit for mapping said at least one of the registration-requested information devices and drivers into the database (Weiss; paragraphs 9-12 and 31-33, discloses user and device information into a database); and

a second list providing unit for providing a list of said at least one of the information devices and drivers registered through the second registration unit based on the multi home service application, with reference to the database (Weiss; paragraph 31, discloses the database is a relational database built on SQL such that if an application requests a list of users and devices registered on the database, the list is provided with reference to the database).

Jung further discloses storing network device information if the multi-home service application transfers a second registration request based on second registration rules provided to register at least one of the other information devices connected to the external home networks and drivers (Jung; Table 1, paragraph 49, and Figures 5 and 12, discloses storing network device information in response to a request to register with a VPN in accordance with a registration request format).

It would have been obvious to one of ordinary skill in the art to modify mapping device information into a database, as disclosed by Weiss, such that the mapping is performed in response to a request, as disclosed by Jung, in order to provide VPN services to an external network or device upon request to register (Jung; paragraph 49).

9. As to Claim 16, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 3. Weiss further discloses wherein if an information device connected to the home network transfers a specific service request for an information device of a specific external home network registered for a service through the multi-home service application, the main processing unit transfers to a destination address of the corresponding information device connected to the home network, a data packet for requesting the specific service to be executed through the VPN tunnel with the specific external home network (Weiss; paragraphs 9-12 and 24-35, discloses facilitating communication between devices through a VPN tunnel over a network which includes transferring service requests between the devices).

10. Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss, Zelig, and Jung as applied to Claim 4 above, and further in view of U.S. Patent No. 5,873,096 to Lim et al. (hereinafter "Lim").

11. As to Claim 5, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 4. Weiss, Zelig, and Jung do not explicitly disclose, however Lim discloses wherein the application processing unit further comprises a setup change unit for, if a deletion and setup change request is transferred from the multi-home service application based on edit rules provided to delete and change a setup of options registered through the first and second registration rules, updating the database based on requested options (Lim; column 6 lines 66-67 and column 7 lines 1-12, discloses updating a database in response to a delete or change request).

It would have been obvious to one of ordinary skill in the art to modify a database, as disclosed by Weiss, to include the functionality to delete or change the database upon request, as disclosed by Lim, in order to provide functionality to update a database (Lim; column 6 lines 66-67 and column 7 lines 1-12).

12. Claims 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss, Zelig, Jung, and Lim as applied to Claim 5 above, and further in view of U.S. Patent No. 7,020,084 B1 to Tanaka et al. (hereinafter "Tanaka").

13. As to Claim 6, Weiss, Zelig, Jung, and Lim in combination disclose each and every limitation of Claim 5. Weiss, Zelig, Jung, and Lim do not explicitly disclose, however Tanaka discloses wherein the application processing unit further comprises a state display unit for, if a state information providing request is transferred from the multi-home service application through a state display window provided to request state information for information exchanges with the external home networks, providing the state information with reference to the database based on whether the VPN tunnel with the external home networks is formed (Tanaka; Figures 6 and 7, column 5 lines 20-50, and column 6 lines 17-25, discloses providing state information with reference to a table based on whether a VPN tunnel is present or absent).

It would have been obvious to one of ordinary skill in the art to modify a database, as disclosed by Weiss, to include maintaining state information regarding a VPN tunnel and providing the state information upon request, as disclosed by Tanaka, in order to provide functionality to control VPN tunnels (Tanaka; column 1 lines 47-51).

14. As to Claim 7, Weiss, Zelig, Jung, Lim, and Tanaka in combination disclose each and every limitation of Claim 6. Weiss further discloses wherein the application processing unit further comprises a service access-allowable range setup unit for, if the multi-home service application sets up and transfers a service accessible range for the information devices connected to the home network and the other information devices based on service accessible range setup rules provided to set up a service accessible range of the external home networks with respect to each of the information devices connected to the home network, mapping transferred service

accessible range setup information into the database (Weiss; paragraphs 9-12, 31-33, and 37, discloses mapping service access information into the database).

15. Claims 8-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss, Zelig, and Jung as applied to Claim 2 above, and further in view of Tanaka and U.S. Patent No. 6,701,437 B1 to Hoke et al. (hereinafter "Hoke").

16. As to Claim 8, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 2. Weiss, Zelig, and Jung do not explicitly disclose, however Hoke discloses wherein the network processing unit comprises:

a network address translation unit for, if a message having a private IP address as an origination address is received from the information devices connected to the home network, translating the private IP address into an authenticated IP address allocated from an ISP, and translating an authentication IP address as a destination address of a message transferred from an external home network into a private IP address allocated to an information device (Hoke; Figure 2, column 8 lines 36-50, and column 9 lines 6-34, discloses translating a private or local IP address as an originating address into an authenticated VPN address and translating an authenticated VPN address as a destination address into a private or local address); and

It would have been obvious to one of ordinary skill in the art to modify processing mutual data exchanges with devices on external networks, as disclosed by Weiss, to include translating a private IP address into an authenticated IP address and translating an authenticated IP into a

private IP address, as disclosed by Hoke, in order to provide means for secure communication (Hoke; column 2 lines 29-37).

Weiss further discloses a VPN processing unit for forming the VPN tunnel through communications with gateways of the external home networks (Weiss; paragraphs 9-12 and 24-35, discloses forming a VPN tunnel to external networks)

Weiss, Zelig, and Hoke do not explicitly disclose, however Tanaka discloses mapping into the database a state of whether the VPN tunnel with the external home networks is formed (Tanaka; Figures 6 and 7, column 5 lines 20-50, and column 6 lines 17-25, discloses a table for mapping the state of whether a VPN tunnel is formed).

It would have been obvious to one of ordinary skill in the art to modify a database, as disclosed by Weiss, to include maintaining state information regarding a VPN tunnel, as disclosed by Tanaka, in order to provide functionality to control VPN tunnels (Tanaka; column 1 lines 47-51).

17. As to Claim 9, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 8. Hoke further discloses the multi-home service system as claimed in claim 8, wherein, if at least one of private IP addresses of the home network and one of the external home networks, wherein the home network and said one of the e home networks constitute two home networks, exist on a same level and one of the two home networks includes the address of the other home network, the network processing unit generates a new network address table for the two home networks to use different private IP addresses in the VPN tunnel

and maps the network address table into the database, and translates, based on one of a new network address table origination and destination addresses, for one of an information device connected to the home network and data packets transferred from the extemal home network (Hoke; column 8 lines 36-50 and column 10 lines 5-20, discloses forming a lookup table for translating data packets transferred between networks).

It would have been obvious to one of ordinary skill in the art to modify processing mutual data exchanges with devices on external networks, as disclosed by Weiss, to include forming a lookup table for translating data packets transferred between networks, as disclosed by Hoke, in order to provide means for secure communication (Hoke; column 2 lines 29-37).

18. As to Claim 10, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 9. Zelig further discloses wherein if the destination address is transferred in a multicast IP address format from an information device connected to the home network, the network processing unit encapsulates the multicast IP address in a data packet used on the Internet (Zelig; column 4 lines 30-53, discloses encapsulating a multicast IP address in a data packet if a destination address is transferred in a multicast IP address format).

It would have been obvious to one of ordinary skill in the art to modify providing mutual access among devices on different networks, as disclosed by Weiss, to include encapsulating a multicast IP address in a data packet if a destination address is transferred in a multicast IP address format, as disclosed by Zelig, in order to provide multicast capability to nodes that are part of a VPN (Zelig; column 4 lines 30-53).

19. As to Claim 11, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 10. Zelig further discloses wherein if a gateway of the one of the external home networks transfers in the multicast format the destination IP address encapsulated in a data packet, the network processing unit multicasts the data packet to the information devices of the home network (Zelig; column 4 lines 30-53, discloses multicasting a received data packet, in a multicast format, to all targeted devices in the VPN)

It would have been obvious to one of ordinary skill in the art to modify providing mutual access among devices on different networks, as disclosed by Weiss, to include multicasting a received data packet to all targeted devices in the VPN, as disclosed by Zelig, in order to provide multicast capability to nodes that are part of a VPN (Zelig; column 4 lines 30-53).

Weiss further discloses if origination and destination IP addresses are transferred in a unicast format from a device packet, transfers the packet in the unicast format to the destination IP address (Weiss; paragraphs 9-12 and 24-35, discloses facilitating communication between devices through a VPN tunnel over a network and thereby discloses transferring packets in a unicast format to a destination address).

20. As to Claim 12, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 11. Weiss further discloses wherein the main processing unit comprises:

a middleware processing unit for collecting device information and service information on the information devices connected to the home network and the other devices, and mapping the device information into the database (Weiss; paragraphs 9-12 and 24-35, discloses collecting user, device, and access information on devices connected to different networks, and mapping the information into a database), and

when an information device connected to the home network requests access to a different information device connected to the home network and the other information devices connected to the external home networks, providing to the access-requesting information device information on the different information device and the information devices connected to the external home networks (Weiss; paragraphs 9-12, 24-35, and 37, discloses providing device specific access information to a device upon request for access); and

a proxy processing unit for exchanging information with the information devices connected to the home network through the middleware processing unit, and exchanging information with the network processing unit to exchange data with the other information devices connected to the external home networks (Weiss; Figure 1, and paragraphs 9-12 and 24-35, discloses exchanging information among devices on a network, and exchanging information among devices on different networks).

21. As to Claim 13, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 12. Tanaka further discloses wherein when an information device connected to the home network transfers a request for an access to at least one of the other information devices connected to the one of the external home networks and no VPN tunnel with

the one of the external home networks is recorded in the database, the middleware processing unit requests the network processing unit to form the VPN tunnel with the one of the external home network (Tanaka; Figures 6 and 7, column 5 lines 20-50, and column 6 lines 17-25, discloses forming a VPN tunnel with an external network when none exists and a request for access to an external network is received).

It would have been obvious to one of ordinary skill in the art to modify a database and request for access to a device, as disclosed by Weiss, to include maintaining state information regarding a VPN tunnel and forming a VPN tunnel with an external network when none exists and a request for access to an external network is received, as disclosed by Tanaka, in order to provide functionality to control VPN tunnels (Tanaka; column 1 lines 47-51).

22. As to Claim 14, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 13. Zelig further discloses wherein if the multicast packets are transferred to the one of the external home networks through the VPN tunnel, the middleware processing unit forwards the multicast packets to the information devices connected to the home network (Zelig; column 4 lines 30-53, discloses transferring multicast packets to all targeted devices in the VPN including devices on different networks).

It would have been obvious to one of ordinary skill in the art to modify providing mutual access among devices on different networks, as disclosed by Weiss, to include multicasting a received data packet to all targeted devices in the VPN, as disclosed by Zelig, in order to provide multicast capability to nodes that are part of a VPN (Zelig; column 4 lines 30-53).

23. As to Claim 15, Weiss, Zelig, Jung, Hoke, and Tanaka in combination disclose each and every limitation of Claim 13. Zelig further discloses wherein if a response message is transferred from an information device having received at least one of the multicast packets, the middleware processing unit transfers the response message to an origination address of the multicast packets through the VPN tunnel (Zelig; Figure 7 and column 4 lines 30-53, discloses including the source IP address in a multicast message along with the destination multicast address such that response messages to a multicast message will be sent to the source IP address).

It would have been obvious to one of ordinary skill in the art to modify providing mutual access among devices on different networks, as disclosed by Weiss, to include multicasting a received data packet to all targeted devices in the VPN and transferring a response to a multicast packet to the origination address, as disclosed by Zelig, in order to provide multicast capability to nodes that are part of a VPN (Zelig; column 4 lines 30-53).

24. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss, Zelig, and Jung as applied to Claim 16 above, and further in view of Tanaka.

25. As to Claim 17, Weiss, Zelig, and Jung in combination disclose each and every limitation of Claim 16. Tanaka further discloses wherein if the VPN tunnel with the specific external home network is not formed, the main processing unit requests the network processing unit to form the

VPN tunnel (Tanaka; Figures 6 and 7, column 5 lines 20-50, and column 6 lines 17-25, discloses forming a VPN tunnel with an external network when none exists).

It would have been obvious to one of ordinary skill in the art to modify a database and request for access to a device, as disclosed by Weiss, to include maintaining state information regarding a VPN tunnel and forming a VPN tunnel with an external network when none exists, as disclosed by Tanaka, in order to provide functionality to control VPN tunnels (Tanaka; column 1 lines 47-51).

26. Claims 18-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Weiss, Zelig, Jung, and Tanaka as applied to Claim 17 above, and further in view of U.S. Patent No. 6,446,200 B1 to Ball et al. (hereinafter "Ball").

27. As to Claim 18, Weiss, Zelig, Jung, and Tanaka in combination disclose each and every limitation of Claim 17. Weiss, Zelig, Jung, and Tanaka do not explicitly disclose, however Ball discloses wherein if a service unaccessible message is received from the specific external home network, the main processing unit updates the database (Ball; column 25 lines 16-45 and column 26 lines 28-47, storing relevant error messages when a service unreachable message is received).

It would have been obvious to one of ordinary skill in the art to modify a VPN system and database, as disclosed by Weiss, to include updating a database when a service unaccessible

message is received, as disclosed by Ball, in order to report network and service errors (Ball; column 25 lines 16-45 and column 26 lines 28-47).

28. As to Claim 19, Weiss, Zelig, Jung, Tanaka, and Ball in combination disclose each and every limitation of Claim 18. Ball further discloses wherein if the service unaccessible message is received from the specified external home network, the main processing unit transfers an unaccessible message to the service-requesting information device (Ball; column 25 lines 16-45 and column 26 lines 28-47, transferring the error reporting service unreachable message to the originator of the request).

It would have been obvious to one of ordinary skill in the art to modify a VPN system, as disclosed by Weiss, to include transferring a service unaccessible message to the originator of the request, as disclosed by Ball, in order to report network and service errors (Ball; column 25 lines 16-45 and column 26 lines 28-47).

29. As to Claim 20, Weiss, Zelig, Jung, Tanaka, and Ball in combination disclose each and every limitation of Claim 19. Weiss further discloses wherein if a data packet requesting a service for an access to an information device connected to the home network is received through the VPN tunnel from an external home network and the external home network is accessible, the main processing unit transfers the data packet to a destination address of the packet (Weiss; paragraphs 9-12, 24-35, and 37, discloses checking the authentication of a data packet received over a VPN tunnel from an external network before transferring the packet to a destination address).

Conclusion

30. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent Application Publication No. 2002/0018456 A1 to Kakemizu et al. – VPN System

31. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to VIVEK KRISHNAN whose telephone number is (571) 270-5009. The examiner can normally be reached on Monday through Friday from 9:00 AM to 5:30 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jason Cardone can be reached on (571) 272-3933. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

VK

/Jason D Cardone/
Supervisory Patent Examiner, Art Unit 2445